УДК 681.324

В.В. МКРТИЧЯН

КОМПЬЮТЕРНЫЕ МОДЕЛИ СПИСОЧНЫХ ДЕКОДЕРОВ ГУРУСВАМИ-СУДАНА ДЛЯ ОБОБЩЕННЫХ КОДОВ РИДА-СОЛОМОНА И КОНКАТЕНИРОВАННЫХ КОДОВ

Решена задача разработки компьютерных моделей списочных декодеров Гурусвами-Судана для обобщенных кодов Рида-Соломона и конкатенированных обобщенных кодов Рида-Соломона с кодами Адамара: разработан точный алгоритм списочного декодирования конкатенированных кодов, получены структурные схемы и программные реализации декодеров.
Ключевые слова: *обобщенные коды Рида-Соломона, конкатенированные обобщенные коды, списочное декодирование*

1. Введение и постановка задачи. Крупным прорывом в теории помехоустойчивого кодирования было создание М. Суданом в 1997 году принципиального списочного декодера для кодов Рида-Соломона (РС-кодов) [1]. Декодер использует интерполяцию и факторизацию многочленов двух переменных над расширением базового поля Галуа и способен с полиномиальной сложностью работать за пределами минимального кодового расстояния. В работе [2] на основе декодера Судана был получен декодер Гурусвами-Судана для обобщенных кодов Рида-Соломона (ОРС-кодов), имеющий лучшие корректирующие способности. В работе [3, с.177] был предложен неформализованный метод списочного декодирования Гурусвами-Судана для ОРС-кодов, специальным образом конкатенированных с кодами Адамара (КОРСА-кодов). Как доказано в [4] списочное декодирование Гурусвами-Судана для ОРС-кодов и КОРСА-кодов можно применить для защиты тиражируемой цифровой продукции от несанкционированного распространения.

В работе [5] программно реализован декодер Судана для РС-кодов. Цель данной статьи – разработка компьютерных моделей списочных декодеров как для более общих ОРС-кодов, так и для КОРСА-кодов. Особенностью представленной разработки является применение в модели списочного декодера для ОРС-кодов длиной r и размерностью k алгоритма факторизации Рота-Руккенштейн [6], позволяющего эффективно, со сложностью $O((\sqrt{rk} + \log q) r \log^2 (r/k))$, проводить факторизацию полиномов двух переменных над полем Галуа F_q.

2. Необходимые сведения об алгоритме списочного декодирования Гурусвами-Судана для обобщенных кодов Рида-Соломона. Пусть F_q – поле Галуа мощностью q; $F_q[x]$ – кольцо полиномов переменной x над полем F_q; $F_q[x,y]$ – кольцо полиномов двух переменных x и y над полем F_q; $F_q^{k-1}[x] \subset F_q[x]$ – пространство полиномов степени не выше $k-1$; $F_q^{\,r}$ – пространство векторов размерностью r над полем F_q; $d(u,v)$ – метрика Хемминга, $u,v \in F_q^{\,r}$ [7]; запись $f \mid p$ далее означает, что f делит p нацело, где $f,p \in F_q[x,y]$. Пусть $\alpha_1,\dots,\alpha_q$ – фиксированное упорядочение элементов F_q; $v_1,\dots,v_r$ – фиксированные элементы $F_q^{\,*}$; $r(\in N) \le q$. ОРС-код длиной r, размерностью k ((r,k)-ОРС-код) можно определить как множество векторов $(v_1 p(\alpha_1),\dots,v_r p(\alpha_r))$, где p пробегает множество информационных полиномов $F_q^{k-1}[x]$.

Алгоритм списочного декодирования Гурусвами-Судана ОРС-кодов [2] включает два основных шага: шаг интерполяции, на котором по полученному слову строится полином двух переменных специального вида, и шаг факторизации, где данный полином разлагается на сомножители, по которым можно построить список. Входными параметрами декодера являются параметры ОРС-кода: мощность поля q, длина r и размерность k кода и некоторый управляющий параметр $t(\in \{\lfloor \sqrt{r(k-1)} + 1 \rfloor;\dots;r\})$. При декодировании на вход алгоритма подается слово $y = (y_1,\dots,y_r) \in F_q^{\,r}$ в виде сетки $\{(\alpha_1,y_1);\dots;(\alpha_r,y_r)\}$. Декодер производит поиск всех кодовых слов в сфере с центром y радиусом $r \cdot t$. Выходом алгоритма является список всех информационных полиномов $f(x)(\in F_q[x])$, удовлетворяющих условию: $|\{i \mid f(x_i) = y_i\}| \ge t$. Из [2] вытекает, что этот список содержит истинное информационное сообщение.

Приведем алгоритм списочного декодирования Гурусвами-Судана для ОРС-кодов в удобном для нас виде

АЛГОРИТМ 1./* Вход: q,r,k,t; сетка $\{(\alpha_1,y_1),\dots,(\alpha_r,y_r)\}$. Выход: список $f(x)$.*/

Шаг 0. Вычислить параметры:

$$m = \left\lfloor (kr + \sqrt{k^2 r^2 + 4(t^2 - kr)})/(2(t^2 - kr)) \right\rfloor + 1 \text{ и } l = mt - 1.$$

Шаг 1. (Интерполяция) Найти любой полином $G(x,y) \in F_q[x,y]$, в виде

$$G(x,y) = \sum_{j_2=0}^{\lfloor l/k \rfloor} \sum_{j_1=0}^{l-kj_2} g_{j_1,j_2} x^{j_1} y^{j_2}, \qquad (1)$$

для которого выполняются следующие условия:

1.

$$\forall i \in \{1;\ldots;r\}\ \forall j_1, j_2 \geq 0:\ j_1 + j_2 < m \Rightarrow$$

$$\sum_{j_1' \geq j} \sum_{j_2' \geq j_2} C_{j_1'}^{j_1} C_{j_2'}^{j_2} g_{j_1', j_2'} x_i^{j_1' - j_1} y_i^{j_2' - j_2} = 0 . \quad (2)$$

2. $G(x, y) \neq 0$.

Шаг 2. (Факторизация) Разложить $G(x, y)$ на неприводимые сомножители.

Шаг 3. Выдать список всех полиномов $f(x) \in F_q[x]$, таких, что $(y - f(x))$ является делителем $G(x, y)$, причем $f(x_i) = y_i$, по крайней мере в t значениях $i \in \{1;\ldots;r\}$.

В [2] также имеется "весовая" версия алгоритма 1, которая, получая на вход параметры (r, k)-ОРС-кода, управляющий параметр $t(\in \{\lfloor \sqrt{k \sum_{i=1}^{r} w_i^2} \rfloor;\ldots;r\})$ и вектор весов $w = (w_1, \ldots, w_r)$ для координат входной сетки $\{(\alpha_1, y_1), \ldots, (\alpha_r, y_r)\}$, находит все информационные полиномы $f(x)$, удовлетворяющие условию $\sum_{i: f(x_i) = y_i} w_i \geq t$. Входная сетка может иметь длину больше r, включая элементы вида: (α, y), (α, y'), где $y \neq y'$, что вместе с весами позволяет учитывать вероятности появления букв y в точке α и строить мягкие декодеры и декодеры для конкатенированных кодов. Алгоритм модифицируется следующим образом: на первом шаге параметр m заменяется на величину $m_i = m\lfloor r w_i / w_{\max} \rfloor$, где $i \in \{1;\ldots;r\}$, $w_{\max} = \max_{i \in \{1;\ldots;r\}} w_i$. Эту версию далее будем называть алгоритмом 1′.

3. Разработка алгоритма списочного декодирования для КОРСА-кодов. В [3, с. 177], изложен метод списочного декодирования Гурусвами-Судана для КОРСА-кодов, однако точного алгоритма декодирования не приводится. В этом разделе построен формализованный алгоритм декодирования.

3.1. Специальное конкатенирование ОРС-кодов с кодами Адамара. Кодирование КОРСА-кодов. Пусть p – простое, m – натуральное, $z_1, \ldots, z_{p^m}$ – фиксированное упорядочение элементов F_p^m. Код Адамара над полем F_p с инициализирующим параметром m задается кодирующим отображением

$$\psi_m : F_p^m \to F_p^{p^m};\ \psi_m(a) = (\langle a, z_1 \rangle, \ldots, \langle a, z_{p^m} \rangle),$$

и имеет минимальное кодовое расстояние $p^m - p^{m-1}$ [7]. Далее этот код будем обозначать как (p^m, m) -А-код.

Для описания специального конкатенирования ОРС-кодов с кодами Адамара введем ряд обозначений. Пусть p – простое, m – натуральное,

$$r \in \{p^m; 2p^m; 3p^m; \ldots; p^{2m}\},\ k \in \{m, 2m, 3m, \ldots, rm / p^m\}, \quad (3)$$

μ_m – биективное отображение, сопоставляющее элементу F_p^m элемент поля F_{p^m} в соответствии с полиномиальным представлением поля,

$$k_0 = k / m,\ r_0 = r / p^m. \quad (4)$$

Рассмотрим биективное отображение:

$$\chi_{m,k} : F_p^k \to F_{p^m}^{k_0 - 1}[x];$$

$$\chi_{m,k}(a) = \mu_m(a^{(0)}) + \mu_m(a^{(1)})x + \ldots + \mu_m(a^{(k_0-1)})x^{k_0-1},$$

где $a = (a_0, \ldots, a_{k-1})$, $a^{(i)} = (a_{im}, \ldots, a_{(i+1)m-1})$, $i \in \{0; \ldots; k_0 - 1\}$.

Очевидно, что отображение $\chi_{m,k}^{-1}$ определяется формулой:

$$\chi_{m,k}^{-1} : F_{p^m}^{k_0-1}[x] \to F_p^k;$$

$$\chi_{m,k}^{-1}(p(x)) = (\mu_m^{-1}(p_0), \mu_m^{-1}(p_1), \ldots, \mu_m^{-1}(p_{k_0-1})),$$

где $p(x) = p_0 + p_1 x + \ldots + p_{k_0-1} x^{k_0-1}$. Рассмотрим отображение:

$$\psi_m^0 : F_{p^m} \to F_p^{p^m};\ \psi_m^0(a) = \psi_m(\mu_m^{-1}(a)),$$

где ψ_m – кодирующее отображение (p^m, m) -А-кода. Пусть $\alpha_1, \ldots, \alpha_{p^m}$ – фиксированное упорядочение элементов F_{p^m}.

КОРСА-код над полем F_p, получаемый специальным конкатенированием (r_0, k_0) -ОРС-кода над полем F_{p^m} и (p^m, m) -А-кода над полем F_p, имеет инициализирующие параметры m, k, r (см. (3), (4)) и задается кодирующим отображением:

$$\gamma_{m,k,r} : F_p^k \to F_p^r;\ \gamma_{m,k,r}(a) = \left(\psi_m^0(p_a(\alpha_1)), \ldots, \psi_m^0(p_a(\alpha_{r_0}))\right),$$

где $p_a(x) \in F_{p^m}^{k_0-1}[x]$ – представление сообщения $a \in F_p^k$ в виде полинома над полем F_{p^m}, служащее для кодирования "внешним" (r_0, k_0) -ОРС-кодом над полем F_{p^m}: $p_a(x) = \chi_{m,k}(a)$; ψ_m^0 – кодирующее отображение "внутреннего" (p^m, m) -А-кода.

КОРСА-код размерностью k длиной r, обозначаемый далее как (r, k) -КОРСА-код имеет минимальное расстояние

$d = (1 - 1/p^m)(1 - (k_0 - 1)/r_0)r$ [3]. Отметим, что в определении КОРСА-кода содержится и метод кодирования.

3.2. Декодирование КОРСА-кодов. Построенный ниже списочный декодер для КОРСА-кодов состоит из двух основных элементов: внешнего и внутреннего. Внешним элементом является "весовая" версия списочного декодера Гурусвами-Судана для ОРС-кодов (см. алгоритм 1′ из раздела 2), а внутренним – списочный переборный декодер кодов Адамара, кратко описанный в [3, с. 181]. Представим последний декодер в формализованном виде.

Входными параметрами списочного переборного декодера кодов Адамара являются параметры (p^m, m) -А-кода над полем F_p : мощность поля *p*, размерность кода m и упорядочение $z_1, \dots, z_{p^m}$ элементов пространства F_p^m . При декодировании на вход алгоритма подается слово $y = (y_i)_{i=1}^{p^m} \in F_p^{p^m}$. Декодер производит перебор всех кодовых слов и составляет список w их "весов по отношению к y ":

АЛГОРИТМ 2: /* Вход: p, m ; $z_1, \dots, z_{p^m}$; y . Выход: w .*/

Шаг 0. Если массив C_a кодовых слов (p^m, m) -А-кода пуст, то рассчитать его элементы: для всех $z_i \in F_p^m$, $i \in \{1;\dots;p^m\}$ вычислить $C_{a,i} = \psi_m(z_i)$; составить $C_a = (C_{a,1}, \dots, C_{a,p^m})$, где ψ_m – определено в 3.1; сохранить C_a для дальнейшего применения.

Шаг 1. Для каждого $z_i \in F_p^m$, $i \in \{1;\dots;p^m\}$ вычислить вес:

$$w_i = \max\{0, 1 - d(y, C_{a,i})/(p^m - p^{m-1})\}.$$

Шаг 2. Составить вектор весов $w = (w_1, \dots, w_{p^m})$ и выдать w .

Имея в наличии все необходимые алгоритмы, построим алгоритм списочного декодирования для КОРСА-кодов. Входными параметрами алгоритма являются параметры КОРСА-кода: параметры полей p и m , длина r и размерность k кода, упорядочения $\alpha_1, \dots, \alpha_{p^m}$ и $z_1, \dots, z_{p^m}$ элементов F_{p^m} и F_p^m соответственно. При декодировании на вход алгоритма подается слово $y = (y_1, \dots, y_r) \in F_p^r$. Декодер производит поиск всех кодовых слов в пределах сферы, центром которой является *y*, радиусом – величина $E = (1 - 1/p^m)(r - \sqrt{rp^m(k/m - 1)})$. Выходом алгоритма является список всех информационных векторов $b (\in F_p^k)$, удовлетворяющих условию: $d(\gamma_{m,k,r}(b), y) \le E$, где $\gamma_{m,k,r}$ – кодирующее отображение (r, k) -КОРСА-кода. Из [3, п.8.4.1] вытекает, что этот список содержит истинное сообщение.

АЛГОРИТМ 3: /* Вход: p,m,r,k :(3); $\alpha_1,\dots,\alpha_{p^m}$, $z_1,\dots,z_{p^m}$; y. Выход: список b.*/

Шаг 0. Вычислить параметры: $q = p^m$, $k_0 = k/m$, $r_0 = r/q$, $t_0 = \left\lfloor \sqrt{r(k-1)} \right\rfloor$, $E = (1-1/q)(1-\sqrt{(k_0-1)/r_0})r$.

Шаг 1. а) Разбить $y = (y_1,\dots,y_r)$ на блоки $y^j \in F_p^{p^m}$: $y^j = (y_{(j-1)q+1},\dots,y_{jq})$, $j \in \{1;\dots;r_0\}$.

б) Для каждого $j \in \{1;\dots;r_0\}$ параметры p, m; $z_1,\dots,z_{p^m}$ и блок y^j подать на вход алгоритма 2; на выходе получить вектор весов $w_j = (w_{j,1},\dots,w_{j,p^m})$.

в) Составить вектор весов $\hat{w} = (w_{1,1},\dots,w_{1,p^m},\dots,w_{r_0,1},\dots,w_{r_0,p^m})$ и

сетку y: $\{((\ _1,\ _1),\dots,(\ _1,\ _{p^m}),\dots,(\ _{r_0},\ _1),\dots,(\ _{r_0},\ _{p^m}))\}$.

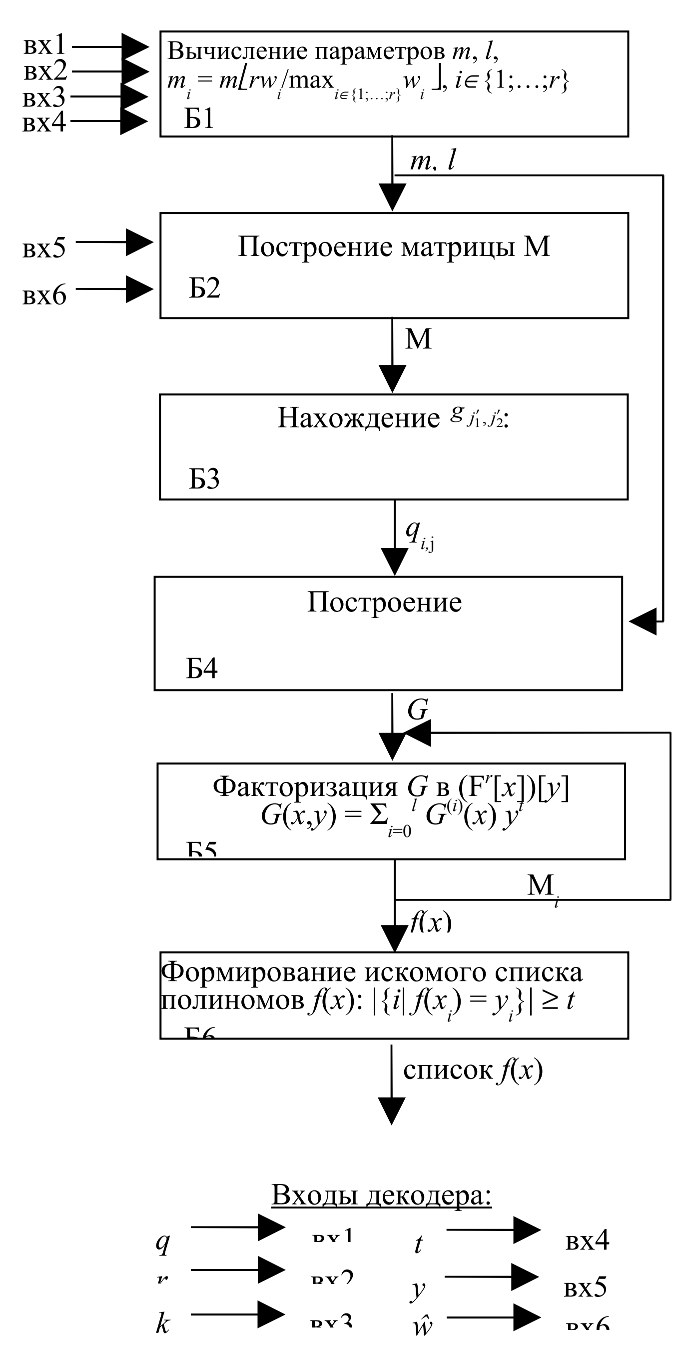
Шаг 2. а) Параметры q,r,k_0,t_0, сетку y и вектор $\hat{w}$ подать на вход алгоритма 1′. На выходе получить список $\{p_1(x),\dots,p_l(x)\}$, где $p_i(x) \in F_{p^m}^{k_0-1}[x]$, $i \in \{1;\dots;l\}$, $l \in N$.

б) Представить полиномы списка $\{p_1(x),\dots,p_l(x)\}$ в виде векторов: $a_i = \chi_{m,k}^{-1}(p_i(x)) \in F_p^k$, где $\chi_{m,k}^{-1}$ – определено в 3.1, $i \in \{1;\dots;l\}$. Выдать список векторов $\{b,\dots,b_{l'}\}$, таких что $d(y,b_i) \le E$, где $b_i \in \{a_1,\dots,a_l\}$, $l' \le l$, $i \in \{1;\dots;l'\}$.

4. Компьютерные модели списочных декодеров.

4.1. Структурные схемы моделей списочных декодеров. На рис.1 и 2 изображены схемы декодеров и системы входов "весовой" версии списочного декодера для ОРС-кодов и списочного декодера КОРСА-кодов. На вход декодера для ОРС-кодов (см.рис.1) подаются: мощность q поля Галуа, длина r и размерность k ОРС-кода, управляющий параметр t, входное слово y и вектор весов $\hat{w}$ помеченные на схеме как ВХ1-ВХ6 соответственно. Декодирование происходит в блоках Б1-Б6. На вход декодера для КОРСА-кодов (рис.2) подаются параметры полей Галуа p и m, длина r и размерность k КОРСА-кода, и упорядочения $\{\alpha_i\}_{i=1}^{p^m}$ и $\{z_i\}_{i=1}^{p^m}$ элементов F_{p^m} и F_p^m соответственно и вектор y, помеченные на схеме как

ВХ1-ВХ7 соответственно. Декодирование происходит в блоках Б1-Б6. Рассмотрим подробнее работу блоков декодеров.



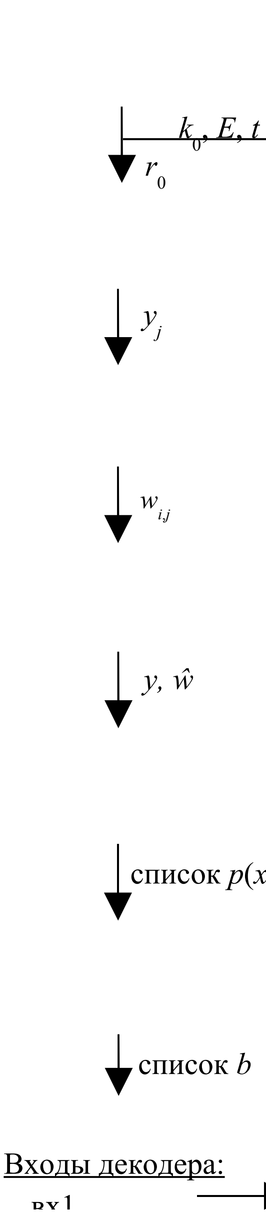


Рис.1. Структурная схема списочного декодера для ОРС-кодов. Схема входов

Декодер КОРСА-кодов

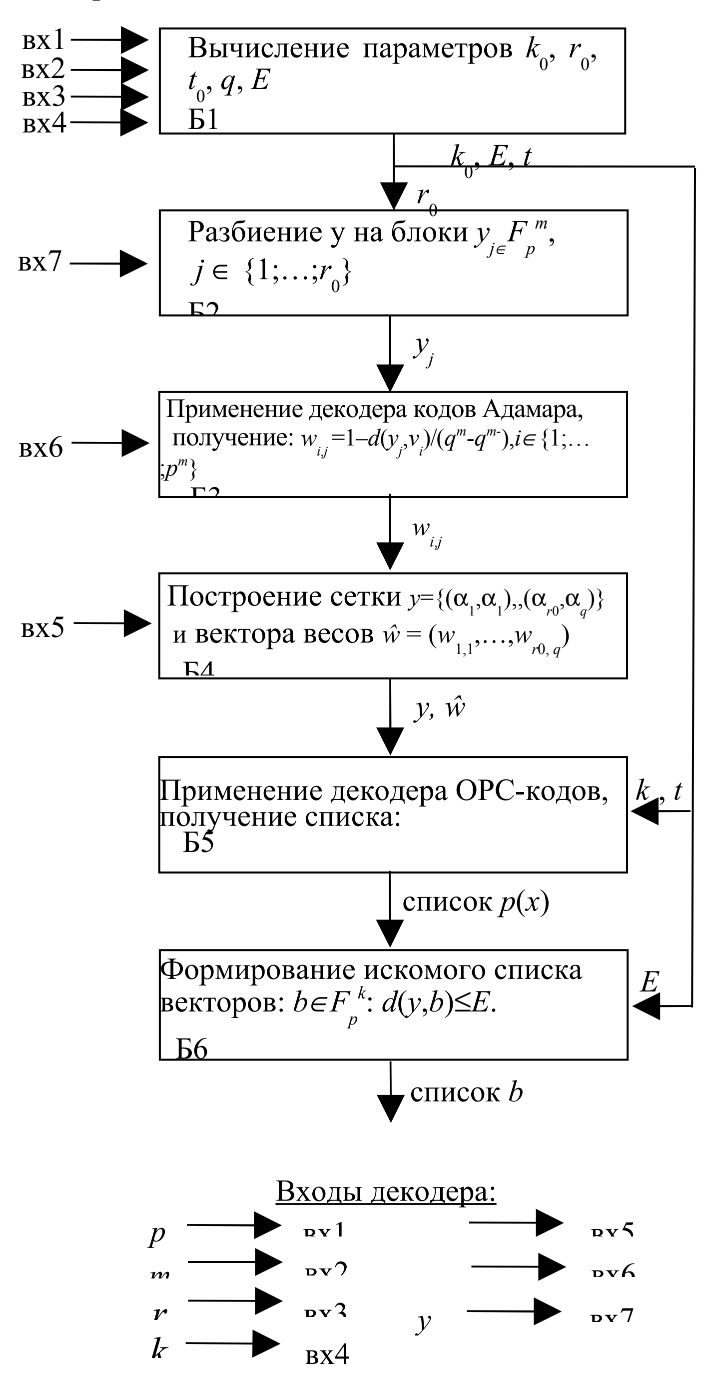


Рис.2. Структурная схема списочного декодера
для КОРСА-кодов. Схема входов

Работа блоков списочного декодера для ОРС-кодов состоит в следующем. Блок Б1 на вход получает q, r, k, t и вычисляет значения параметров декодера l, m и $m_i = m\lfloor rw_i / \max_{i\in\{1;\ldots;r\}} w_i \rfloor$, для $i \in \{1;\ldots;r\}$. Блок Б2 на вход получает l, m_i и строит матрицу однородной системы (2), обозначенную на схеме буквой М. Построение i-й строки происходит путем вычисления коэффициентов $(x_i)^{j_1'-j_1}(y_i)^{j_2'-j_2}$ при неизвестной $g_{j_1',j_2'}$ ($(x_i, y_i) \in \{(x_1, y_1),\ldots,(x_r, y_r)\}$) и присвоения их координатам строки. При этом порядок следования элементов строки несущественен, но в реализации проще использовать естественный порядок, получаемый при раскрытии двойной суммы. Блок Б3 на вход получает матрицу M и решает матричную систему $M\overline{g} = 0$ методом Гаусса, где $\overline{g}$ – вектор-столбец коэффициентов $g_{j_1',j_2'}$ полинома (1), находит коэффициенты $g_{j_1',j_2'}$. Блок Б4 получает на вход l, m_i, коэффициенты $g_{j_1',j_2'}$ и строит полином (1). Блок Б5 реализует рекурсивную процедуру факторизации полинома (1) на основе алгоритма Рота-Руккенштейн. Процедура в процессе работы строит дерево коэффициентов полиномов, ветви которого образуют список элементов, включающий искомый. Блок Б6 кодирует полиномы списка выхода Б5, и формирует искомый список.

Работа блоков списочного декодера для КОРСА-кодов состоит в следующем. Блок Б1 на вход получает p, m, k, r, вычисляет значения параметров декодера $k_0, r_0, t_0 = \lfloor\sqrt{r(k-1)}\rfloor, q, E$. Блок Б2 на вход получает r_0 и y, разбивает y на блоки y_j, $j \in \{1;\ldots;r_0\}$ для обработки алгоритмом 2. Блок Б3 реализует алгоритм 2, вычисляя по полученным на вход блокам y_j и упорядочению $\{z_i\}_{i=1}^{p^m}$ веса $w_{i,j}$, где $i \in \{1;\ldots;p^m\}$, $j \in \{1;\ldots;r_0\}$. Блок Б4, получая на вход веса $w_{i,j}$ и упорядочение $\{\alpha_i\}_{i=1}^{p^m}$, формирует вектор весов $\hat{w}$ и строит сетку y. Блок Б5, получая на вход y, $\hat{w}, k_0, t$ применяет алгоритм 1′ и получает список полиномов $p(x) \in F_{p^m}^{k_0-1}[x]$. Блок Б6 получает на вход список полиномов и величину E, представляет полиномы в векторном виде и формирует искомый список.

4.2. О программной реализации. Рассмотрим аспекты программной реализации приведенных структурных схем. Вычисления в полях Галуа, векторных пространствах и кольцах полиномов над полями Галуа реализованы на языке С++ на базе динамической библиотеки WinNTL-5_4_1 (см., например, [8]), включающей классы алгебраических структур и алгоритмов, необходимых для реализации моделей, таких как класс расширения поля Галуа, класс полиномов над полем и другие. Недостающие структуры и алгоритмы получены в программной реализации в виде отдельных классов, например, кольцо полиномов с коэффициентами из кольца полиномов над полем Галуа.

На основе полученной в предшествующей работе [5] реализации списочного декодера Судана для РС-кодов и указанных базовых компонен-

тов построены новые классы, реализующие рассмотренные структурные схемы декодеров. Для тестирования их работоспособности и постановки экспериментов получены реализации вспомогательных классов.

Класс декодера Гурусвами-Судана для ОРС-кодов получен как наследник класса списочного декодера Судана, включающий виртуальные процедуры создания улучшенной интерполяционной матрицы Гурусвами-Судана и обеспечения корректной работы с полями базового класса и класса-наследника с учетом специфики данного декодера. Класс декодера для КОРСА-кодов включает декодеры для ОРС-кодов и кодов Адамара как поля класса.

Структурные схемы реализованы программно на основе библиотеки MFC под следующие операционные системы: Windows 95/98/NT/2000/XP/Vista.

Построенная программная реализация декодеров использована для проведения численных экспериментов в связи с применением списочного декодирования в схеме специального широковещательного шифрования [9], где имеет смысл использовать коды с относительно большим кодовым расстоянием. Так, например, при декодировании 140 слов (37,2)-ОРС-кода над полем F_{37} при числе ошибок в канале, не превышающем 70%, получены списки объемом в одно кодовое слово, а в случае, когда число ошибок составляло 70% – 81%, списки состояли из двух кодовых слов. Если число ошибок превышает 81%, то декодер не гарантирует правильное декодирование, так как при наших параметрах количество гарантируемо исправляемых ошибок равно $\lceil r - \sqrt{r(k-1)} - 1 \rceil$ = 30 (см. раздел 2.). Декодирование 140 слов производилось программой в течение двенадцати секунд на компьютере с процессором мощностью 2,5 ГГц и ОЗУ объемом 512 Мб. Из [9] вытекает, что рассмотренный пример ОРС-кода в схеме специального широковещательного шифрования соответствует тиражу легально распространяемой продукции, равному 1369 экземпляров, а декодирование каждого слова гарантирует нахождение распространителей обнаруженного экземпляра контрафактной продукции.

5. Заключение. Решены задачи разработки компьютерных моделей списочных декодеров Гурусвами-Судана для ОРС-кодов и КОРСА-кодов с использованием эффективного алгоритма факторизации Рота-Руккенштейн. Для их применения в цифровых системах передачи данных к разработанной схеме можно добавить блок, реализующий выделение истинного сообщения из списка на выходе декодера [10]. На основе результатов, полученных в настоящей работе, возможно расширение компьютерной модели схемы специального широковещательного шифрования, построенной автором данной статьи в [9]. Отметим, что в настоящее время специалистами ведутся интенсивные теоретические исследования по оптимизации времени работы всех этапов списочного декодирования (см., например, [3], [11]). Разумеется, применение этих результатов в технической реализации декодеров должно привести к улучшению их временных характеристик.

Библиографический список

1. *Sudan M.* Decoding of Reed Solomon codes beyond the error-correction bound/ M. Sudan // Journal of Complexity, 1997, v. 13, n. 1, p. 180-193.

2. *Guruswami V.* Improved decoding of Reed-Solomon and algebraic-geometric codes/ V.Guruswami, M.Sudan // IEEE Trans. Inf. Theory, 1999, v. 45, p. 755-764.

3. *Guruswami V.* List Decoding of Error-Correcting Codes / V.Guruswami. – New York: Springer-Verlag Inc. (LNCS 3282), 2005, 350 p.

4. *Silverberg A.* Application of list decoding to tracing traitors / A.Silverberg, J.Staddon, J.Walker. In Adv. in Cryptology - ASIACRYPT 2001 (LNCS 2248), 2001, p. 175-192.

5. *Мкртичян В.В.* О реализации программного модуля детерминированного списочного декодера Судана для кодов Рида-Соломона / В.Мкртичян // Вестник ДГТУ, 2007, т.7, №3. – С. 270-275.

6. *Roth R.*. Efficient decoding of Reed-Solomon codes beyond half of minimum distance/ R.Roth, G.Ruckenstein // IEEE Trans. on Inf. Theory, 2000, v. 45, p. 432-437.

7. *Мак-Вильямс Ф.Д.* Теория кодов, исправляющих ошибки / Ф.Д.Мак-Вильямс, Н.Дж.Слоэн. – М.: Связь, 1979. – 744 с.

8. Библиотека классов WinNTL-5_4_1. http://shoup.net/ntl/.

9. *Мкртичян В.* Компьютерная модель схемы специального широковещательного шифрования на основе кодов Рида-Соломона и списочного декодера Гурусвами-Судана /В.Мкртичян // Материалы IX Международной науч.-практ. конф. "Информационная безопасность". Ч.2. – Таганрог: ЮФУ, 2007. – С. 111-115.

10. *Маевский А.Э.* Об экспериментальном исследовании списочного декодера Судана для кодов Рида-Соломона / А.Э.Маевский, В.В.Мкртичян // Компьютерные технологии в науке и производстве. Мат-лы V НТК., часть 3, ЮРГТУ(НПИ), 2004. – С. 29-30.

11. *Трифонов П.В.* Интерполяция в списочном декодировании кодов Рида-Соломона / П.В. Трифонов // Проблемы передачи информации, 2007. – Т. 43. – Вып. 3. – С.66-74.

Материал поступил в редакцию 12.12.07.

V.V.MKRTICHAN

COMPUTER MODELS OF SUDAN AND GURUSWAMI'S LIST DECODERS FOR GENERALIZED REED-SOLOMON CODES AND CONCATENATED CODES

Problem of computer model development of Sudan and Guruswami's list decoders for generalized Reed-Solomon codes and concatenated codes is solved. Strict algorithm of list decoding of concatenated codes is given. The block diagram and program realization of decoder are constructed.

МКРТИЧЯН Вячеслав Виталиевич (р.1982), окончил магистратуру кафедры "Программное обеспечение вычислительной техники и автоматизированных систем" ДГТУ, аспирант.
Основные научные интересы – математические методы в системах защиты информации.
Автор 9 публикаций.